Algebraic Structures :

Well Ordering Principle : Every nonempty set of positive integers contains a smallest member.

Division Algorithm (Euclid) : Let a and b be integers with $b > 0$. Then there exist unique integers q and r with the property that $a = bq + r$ where $0 \le r < b$.

Fundamental Theorem of Arithmetic : Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear.

Binary Operation : Let G be a nonempty set. An operation on G is a function $*$ from $G \times G$ into G is called Binary operation.

We usually write $\underline{a * b}$ or $\underline{ab}$ instead of $*(a, b)$.

The combination of G and $*$ is called algebraic structure (system) and written as $(G, *)$.

e.g. The addition is a binary operation on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Therefore, $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are algebraic systems.

[Suppose S is a set with an BO $*$ and suppose A is a subset of S. Then A is said to be closed under $*$ if $a * b \in A$ $\forall\, a, b \in A$

$\therefore$ A BO $*$ ~~fo~~ on a set A is same A is closed under $*$.]

The set of irrationals numbers is not ~~closure~~ closed under multiplication.

Semigroup: Let G be a nonempty set and $*$ is a BO on G. Then $(G, *)$ is called Semigroup if

(i) G is closed under $*$. (Closure law)

(ii) $*$ is an associative operation (Associative law).

e.g. Consider (Σ^*, concatenation) where Σ^* is an alphabet. Σ^* is closed with respect to concatenation and concatenation is an associative operation. Therefore (Σ^*, concatenation) is a semigroup

$\boxed{(\mathbb{Z}, -) \text{ is not semigroup}}$

Monoid: Let G be a nonempty set and $*$ is a BO on G. Then $(G, *)$ is called Monoid if

(i) G is closed under $*$

(ii) $*$ is an associative operation

(iii) There exists an identity element $e \in G$ for $*$.
i.e. for any $x \in G$, $e * x = x * e = x$

e.g. $(\mathbb{Z}, +)$ is monoid as $\mathbb{Z}$ is closed under addition, addition is associative and 0 is identity element.

$(\mathbb{N}, +)$ is not monoid but Semigroup.

Group: Let G be a nonempty set together with a binary operation $*$ is called a <u>group</u> if

(i) G is closed under $*$

(ii) $*$ is an associative operation

(iii) $(G, *)$ has an identity element

(iv) For each element a in G, there is an element b in G such that $a*b = b*a = e$.